UTAH DEPARTMENT OF HUMAN SERVICES POLICY AND PROCEDURES		
Reference: 06-04	**Effective Date: October 20, 1997** **Revision Date: June 3, 2013**	**Page 1 of 10**
SUBJECT: POLICY ON THE APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES		
RATIONALE: The purpose of this policy is to ensure that information technology resources ("IT Resources") owned or operated by the State of Utah or the Utah Department of Human Services are used efficiently and appropriately. This policy is also designed to notify Department employees and others about how they may (and may not) use IT Resources, and about how the Department will monitor and enforce this policy.		

1. **Department's Policy Regarding the Appropriate Use of IT Resources:** It is the policy of the Utah Department of Human Services (the "Department") that IT Resources are valuable government resources that must be used efficiently and appropriately to carry out the business of the State of Utah (the "State") and the Department. The Department will monitor and enforce this policy to ensure that its employees and other users do not use IT Resources for impermissible personal uses or for any other uses that violate this policy.

2. **Scope of This Policy:** This policy supplements any statutes, rules and policies established by the State, including: (a) Rule 365-7 on "information technology protection"; and (b) "acceptable use" policies adopted by the State's Chief Information Officer pursuant to Utah Code Ann. § 63D-1a-301.

3. **Definitions Used in This Policy:**

   a. **"IT Resources"** means a wide range of information technology resources owned or operated by the State or the Department, including:

      (1) Computer hardware. The physical components of a computer system and related devices. Examples of hardware include motherboards, disk drives, memory, monitors, keyboards, mice, printers, and scanners;

      (2) Computer software. A set of instructions that cause a computer to perform one or more tasks. Computer software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system. Three main types of software are system software, application software, and information systems:

         a. System software. Programs and processing routines that control a computer's internal functioning, chiefly through an operating system, and also controls such peripherals as monitors, printers, mice and storage devices. Examples of system software include operating systems (Windows, Linux, UNIX, NetWare) and utility programs (sort, merge, backup);

         b. Application software. Programs designed to handle specialized tasks; many of which are sold or licensed as ready-to-use packages. Examples of application software include general-purpose spreadsheet and word

processing programs, Internet browsers, programming languages (Basic, C++, Java, PowerBuilder); and

c. Information systems. An integrated set of programs and organized procedures for collecting, storing, processing, communicating information, decision making, and control in the organization. Information systems are tailored to meet the unique business requirements of the organization. Examples of information systems include CARE, Data Warehouse, Echart, FINET, HRE, ORSIS, Payroll, SAFE, SAMHIS, USSDS, and USTEPS;

(3) Electronic mail ("e-mail");

(4) Electronic voice and video communications (including voice mail):

(5) Information storage media (including hard disks, floppy disks, zip disks and the electronic files and records contained on those disks);

(6) Telecommunications equipment;

(7) Facsimile equipment and facsimiles (often called faxes);

(8) The Internet;

(9) Logs or similar records that indicate Internet use or access, and information downloaded from the Internet; and

(10) Future technologies owned, provided or operated by the State or the Department.

NOTE: All items listed in the definition of "IT Resources" are the property of the State and the Department. Under state and federal law, files and other contents of these IT Resources may be regarded as "records" of the State or the Department. For example, depending on its content, an e-mail message may be a "record" under GRAMA (Utah's Government Records Access and Management Act).

b. **"User"** of IT Resources means all Department employees, volunteers, contract providers and others who have accessed or who currently have access to IT Resources.

c. **"Use"** means any use of IT Resources. The term "use" shall be broadly interpreted to include such activities as preparing, sending, accessing, viewing, retrieving, downloading, faxing, copying and printing documents, files and programs, or using telecommunication resources such as phones and faxes.

d. **"Computer Virus"** means any program that can destroy application software or data files, or which can disrupt the operation of IT Resources. (IT Resources can be contaminated by viruses in many ways, including downloading files from the Internet, using pirated (unlicensed) software, and opening email attachments that contain viruses.)

e. **"Personal Use"** means any use of IT Resources that is not reasonably relevant or applicable to the User's job-related duties for the Department. "Personal Use" includes such activities as correspondence (electronic or otherwise), games, transactions (including sales and purchases), calculations, downloading or accessing information, and other commercial, social, charitable, religious, political or recreational activities that are not related to the User's job.

f. **"Monitor"** means to access, observe, review, audit, intercept and disclose a User's use of IT Resources. Monitoring may be random or may be focused on a specific User.

4. Uses of IT Resources.

a. **Unauthorized Uses of IT Resources:** The following uses of IT Resources are always prohibited:

(1) Illegal, Disruptive, Inefficient, Destructive or Risky Uses: Users may not use IT Resources to engage in any activity that:
   a. violates federal, state or local statutes, regulations or policies;
   b. disrupts or distracts from the conduct of State or Department business;
   c. reduces job productivity, or unreasonably expends the resources of the State or the Department;
   d. alters, destroys, dismantles or disfigures IT Resources;
   e. creates a security risk to IT Resources, or disrupts the use or performance of IT Resources; or
   f. involves the storage of unauthorized data or software on IT Resources;

(2) **Private Business Uses**: A User may not use IT Resources to run a private business or engage in conduct related to the User's personal enterprises or commercial activities, including the preparation or transmittal of any correspondence, records, billings, advertisements or solicitations related to such activities;

(3) **Religious or Political Uses:** A User may not use IT Resources to prepare or send any religious or political communications, including correspondence, petitions, brochures, tracts, position statements or announcements, if those

communications involve proselytizing, solicitation, lobbying, advertising, fund-raising or more than minimal use of the Department's resources;

(4) **Sexually Explicit or Pornographic Uses:** A User may not use IT Resources to access, review, send, retrieve or print any sexually explicit or pornographic material (regardless of whether it is pictorial or textual, and regardless of whether it is technically "obscene" under state and federal laws) unless the material is reasonably relevant to and necessary for the performance of the User's job-related duties. The User shall have the burden of proving that any such use was reasonably relevant to and necessary for the performance of the User's job-related duties, unless the User obtains prior written approval from the User's supervisor, authorizing such access or use of sexually explicit or pornographic material, and unless the supervisor files a copy of such approval in the User's personnel file or contract file;

(5) **Illegal Copying or Pirating:** A User may not use IT Resources to copy, send, "pirate" or use software, copyrighted materials or another person's original writings or programs, in violation of copyright license agreements or laws;

(6) **Inappropriate Access to Confidential or Restricted Material:** A User may not use IT Resources to access information which is classified or treated as confidential or otherwise restricted, unless the User is authorized to access such information under applicable laws, statutes, regulations or policies;

(7) **"Hacking" and Other Forms of Unauthorized Access:** A User may not use IT Resources to access or "hack" into unauthorized files, programs, applications or other IT Resources, or to obtain access to any IT Resources to which the User has no job-related need or for which the User is not authorized to access;

(8) **Masquerading As Another User**: A User may not use IT Resources to masquerade as another User, or to read, examine, disclose, copy or alter the personal files of another User, unless such activities are: (a) authorized by the User; or (b) approved by the User's supervisor and permitted by state or federal law or this policy;

(9) **Harassment:** A User may not use IT Resources to send information that may reasonably be interpreted as harassment of others based on race, national origin, sex, sexual orientation, age, disability, religion, or political affiliation;

(10) **Spreading Computer Viruses:** A User may not use IT Resources to knowingly or negligently spread a computer virus;

(11) **Junk Mail:** A User may not use IT Resources to distribute "junk" mail such as chain letters, advertisements or solicitations;

(12) **Inappropriate Use of Printers**: A User may not use a Department printer for personal use or for large print jobs which could be done less expensively and more efficiently by using available photocopiers or offset presses; or

13) **Careless Use of Confidential Information**: A User may not use IT Resources to send confidential or otherwise-restricted information without taking proper precautions (such as encryption) to ensure that the transmission is secure. (The Governmental Records Access and Management Act ("GRAMA") and many other state and federal laws restrict public access to certain records, including electronic records, maintained by the Department.)

b. **Penalties for the Unauthorized Use of IT Resources:** The unauthorized use of IT Resources may result in one or more of the following: removal of privileges to IT Resources; corrective action or disciplinary action (including termination) in accordance with the State's Human Resource Management Rules; civil action; and criminal prosecution under state or federal laws and regulations regarding the use of IT Resources. See, e.g., The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 1367 et. seq.), the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030 et. seq.), the Utah Computer Crimes Act (Utah Code Ann. § 76-6-701 et. seq.), rules regarding "Information Technology Protection" (Utah Admin. Code R895-7-4 et. seq.), and rules of the Utah Department of Human Resource Management, Utah Admin. Code 477-9-6.

(1) **"Zero Tolerance" for Pornography and Sexually Explicit Materials:** The Department has "zero tolerance" for using IT Resources to access or transmit pornographic materials in violation of this policy, and such uses will result in termination of the User's employment or contract with the Department. Using IT Resources to access or transmit sexually explicit materials may also result in termination, depending on the nature of the material.

c. **Personal Use of IT Resources:** IT Resources may be used only in conjunction with a User's job-related duties, except as provided in this section. Frequent or extensive non-job-related use of IT Resources reduces job productivity, and is not permissible. However, certain incidental and occasional Personal Use of IT Resources is permitted during lunch or break periods or for short periods of time before or after regular working hours, as long as such use does not:

(1) Involve an Unauthorized Use of IT Resources (see Section (4)(a) above);

(2) Have the potential to embarrass the State or the Department;

(3) Involve generalized or widespread publication or disclosure of a Department-based (or State-based) e-mail address or similar identifying information, such as can occur when a User sends jokes to a large number of friends by e-mail, or when a User accesses an electronic chat room, an electronic bulletin board or an electronic auction service;

(4) Involve sending or receiving frequent or numerous non-job-related messages (such as e-mails, faxes or advertisements);

(5) Incur a cost that the User must reimburse to the State or the Department, unless the Department has authorized such use and reimbursements in advance; or

(6) Involve the storage of more than 20 megabytes (MB) of data on the Department's hard drives or network.

Examples of Permissible and Non-Permissible Personal Uses:

- A User may make an occasional purchase from an on-line catalog such as Lands' End during the User's break times, as long as the merchandise is delivered to the User's home, and as long as the User does not authorize Lands' End to send advertisements or other materials to the User's e-mail address at the Department.

- Even during lunch or break times, however, a User may not use IT Resources to participate in a recreational chat room or an electronic auction such as e-Bay.

- A User may never access pornographic material or order anything from an on-line source that offers sexually explicit material, unless a supervisor gives prior written approval in accordance with Section (4)(a)(4) above.

- A User may use IT Resources during the User's break times to type up a small calendar events for the User's church group, but a User may not use IT Resources to prepare a proselytizing brochure or a fund-raising letter for the church group.

- A User may not use IT Resources to receive regular or automated investment information or announcements about airline ticket prices.

NOTE: This list of examples is intended to help Users understand the policy on IT Resources. It is not intended as an exhaustive list of permissible and non-permissible Personal Uses.

5. **Mobile Computing Devices:** The use of mobile computing devices such as laptops, cell phones, smart phones, digital recording devices, thumb drives, or any device capable of storing data must be protected from being lost or stolen. The following list will be helpful in preventing such loss.

   a. Mobile computing devices that contain Personal Identifiable Information (PII) or sensitive information from state systems should be password protected and encrypted so stored information won't be compromised if the device is lost or stolen.

   b. Only approved State owned mobile devices that are password protected and encrypted should be used for storing for state data. (DTS will assist in obtaining the appropriate devices).

   c. Mobile computing devices that contain PII or sensitive information should be physically secured at all times:

      (1) Never leave a mobile computing device in an unattended vehicle where it can be seen. Such devices should be locked in the trunk.

      (2) Never leave a mobile computing device overnight in an unattended vehicle.

      (3) Hand-carry or keep mobile computing devices under visual observation while traveling on public transportation.

      (4) Use a cable lock to anchor laptops to a fixed object in the room during hotel stays.

      (5) Do not leave a mobile computing device in an unattended, unsecured personal residence.

      (6) Do not leave a mobile computing device unattended and unsecured in the workplace. Unless in a locked office, mobile computing devices should be locked in a container or secured with a cable lock to an immovable object.

   d. If a mobile computing device is lost or stolen the incident must be reported to the supervisor and the Office/Division Director within one business day of becoming aware of the incident.

6. **Monitoring of IT Resources**: The Department has the right, at its discretion, to monitor its IT Resources to ensure that they are being used appropriately and are functioning properly. See, e.g., Utah Admin. Code R895-7-4 et seq. This means that the Department may monitor a User's individual use of IT Resources (including e-mail messages and other documents) for any reason without notifying the User in advance. Although this policy allows Users to engage in certain Personal Uses of IT Resources, Users do not have any expectation that they can use such IT Resources free of the Department's monitoring or scrutiny.

7. **Reporting of Unauthorized Use of IT Resources:** Any User who receives a complaint or otherwise becomes aware of an Unauthorized Use of IT Resources shall report this information to the appropriate Human Resource Specialist in the Department's Office of Human Resources. The Human Resource Specialist will work as needed with representatives of management, the Department

   Technology Services and the Bureau of Internal Audit and Review to investigate the nature and extent of the alleged Inappropriate Use, and shall submit findings to management.

8. **Appropriate Choice of IT Resources**: Users must exercise good judgment about when and how they use IT Resources. For example, sending an e-mail message creates a written record of your communication, and e-mails are easily forwarded (inadvertently or intentionally) to recipients other than the ones you intended. This can lead to awkward situations for you and the Department. Similarly, firing off an indiscreet or angry e-mail message can create a whole host of difficult problems for you and the Department. Users also need to remember that various federal and state laws (such as GRAMA) may require agencies and individuals to disclose certain records, including electronic records such as e-mail, faxes, word processing documents, pagers, and the Internet. Moreover, in some cases, the Department may be required to disclose e-mail messages or computer documents to the opposing party in a lawsuit. With this in mind, Users of IT Resources should be aware of the value and sensitivity of information produced by their IT activities, and they should give adequate consideration to selecting an appropriate method of using, storing or delivering each message or information.

9. **Additional Software:** Users may install and maintain additional commercial software (i.e., software that is not provided by the State or the Department) on their workstations only if:

   a. Installing or using the software complies with all licensing and copyright laws, and the User has retained documentation showing that the User owns or is licensed to use the software;

   b. The software supports a job-related function;

c. The User has obtained the Department's or Division's approval before installing the commercial software; and

d. The User's supervisor files a copy of this approval in the User's personnel or contract file.

10. Procedures for Accessing IT Resources:

a. **DHS Network Access Request Form:**

(1) All Users of IT Resources shall sign the DHS Network Access Request Form, certifying that they have read and will comply with the DHS Policy on the Appropriate Use of Information Technology Resources. The DHS Network Access Request Form shall contain the following statement:

I have read, understand and agree to comply with the Department's "Policy on the Appropriate Use of Information Technology Resources." I have discussed any questions and issues of concern with my supervisor or contract manager in the Department, and these matters have been resolved to my satisfaction.

User's Signature: _____ Date: _____

(2) A new User may not obtain access to IT Resources until that User and his/her supervisor have signed the DHS Network Access Request Form.

(3) The Department may periodically require Users and their supervisors to complete the DHS Network Access Request Form re-certifying that they understand and will comply with the DHS Policy on the Appropriate Use of Information Technology Resources.

(4) The User's supervisor shall maintain the completed DHS Network Access Request Forms in the User's Human Resources (HR) file or contract file.

b. **User Accounts:** The Department of Technology Services (DTS), Security Group or Help Desk shall not establish a User account for any person who requires access to an information system until that user and his/her supervisor have signed the appropriate authorization form for that information system. The User's supervisor shall evaluate the User's job responsibilities and determine the appropriate level of access to the information system, based on a "need to know/need to do" factors. The supervisor shall submit the completed authorization form to DTS, the Security Group or Help Desk

c. indicating the level of access required to carry out the User's job. DTS, the Security Group or Help Desk responsible for creating a User account shall maintain the completed access request form in their office.

d. **Password and Access Security**:

(1) Users are responsible for maintaining the security of their passwords. Users may not share, post or display their logon id's or passwords.

(2) Passwords shall be at least six characters long.

(3) Passwords shall be changed at least once every ninety (90) days, or more frequently if the User requests.

(4) Users shall change their passwords whenever a security problem is identified by the User or the Division or the Department of Technology Services.

(5) Each account shall have six (6) grace logons before the account is locked. The Department of Technology Services will unlock a User's account only if a satisfactory response is received from the User about the failed attempts.

d. **Security Procedures When a User Transfers or Leaves the Department**: The User's supervisor or contract manager shall collect all IT Resources assigned to the User and shall ensure that access to IT Resources is terminated. The supervisor or contract manager shall notify DTS, the Security Group or Help Desk to close the user's account.

An "exit interview form" may be used for this purpose, and can be obtained from the following on-line site: http://www.hsemployees.utah.gov/ot/forms/exitinte.pdf.

Palmer DePaulis DATE 6/5/2013

Palmer DePaulis, Executive Director
Department of Human Services